

ORIGINAL

NORTHERN DISTRICT OF TEXAS
FILED

IN THE UNITED STATE DISTRICT COURT, 3
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

CLERK, U.S. DISTRICT COURT

By Deputy

LIQUID MOTORS, INC.

CAUSE NO. 3:09-cv-0611-N

v.

ALLYN LYND AND
UNITED STATES OF AMERICA

§
§
§
§
§
§
§

**FIRST AMENDED COMPLAINT,
APPLICATION FOR TEMPORARY RESTRAINING ORDER, MOTION FOR RETURN
OF PROPERTY AND BRIEF IN SUPPORT**

Liquid Motors, Inc. ("Liquid Motors") files this First Amended Complaint, Application for Temporary Restraining Order, Motion for Return of Property and Brief in Support and respectfully shows the Court as follows:

INTRODUCTION

Liquid Motors provides electronic inventory management and marketing services to national automobile dealers. Liquid Motors provides these electronic services through computer servers and other equipment, located at 2323 Bryan Street, Dallas, Texas (the "Building"). On April 2, 2009, the Federal Bureau of Investigation ("FBI") raided the Building. The FBI seized all of the servers and equipment belonging to Liquid Motors. As a result, Liquid Motors has been put out of business for the time being and is unable to provide services to its clients throughout the country.

Meanwhile, there is no reason to believe that the data contained on Liquid Motors' storage arrays, servers, and other equipment has anything more than a remote chance of furthering the government's investigation.

Over 750 clients rely on Liquid Motors for their internet marketing services. If Liquid Motors cannot get its equipment back up and running immediately, it will lose its customers and will go out of business for good.

PARTIES, JURISDICTION, AND VENUE

1. Plaintiff Liquid Motors, Inc. is a citizen of the State of Delaware and is incorporated under the laws of the State of Delaware. Liquid Motors maintains its home office and principal place of business in Richardson, Texas.

2. Defendant Allyn Lynd is a Special Agent of the Federal Bureau of Investigation. Upon information and belief, Defendant Allyn Lynd seized the computer equipment at issue in this case.

3. Defendant United States has been named in this action. Copies of this amended application have been provided to the United States Attorney's Office in Dallas by email.

4. This Court has jurisdiction of this action under 28 U.S.C. § 1331 because this case arises under the law of the United States.

5. Venue of this action is proper in the Northern District of Texas, Dallas Division, under 28 U.S.C. Section 1391(a)(2) because a substantial portion of the events giving rise to these claims occurred in the Northern District of Texas, Dallas Division.

FACTUAL ALLEGATIONS

6. Liquid Motors provides electronic inventory management and internet marketing services to national automobile dealers. Liquid Motors provides these electronic services through computer servers and two storage arrays, which are located at 2323 Bryan Street, Dallas, Texas (the "Building").

7. Upon information and belief, this Court issued a search warrant to Special Agent Allyn Lynd of the FBI to seize computer equipment in pursuit of an ongoing investigation.

8. On April 2, 2009, the Federal Bureau of Investigation ("FBI"), upon information and belief, raided the Building under a search warrant issued for 2323 Bryan St., Dallas, Texas.

9. Although, upon information and belief, the search warrant was not issued for any alleged wrongdoing by Liquid Motors, the FBI seized all of the servers and backup tapes belonging to Liquid Motors.

10. Since the FBI seized its computer equipment earlier today, Liquid Motors has been unable to operate its business.

11. Liquid Motors' business is to provide ongoing inventory management and internet marketing services to automobile dealerships throughout the country. Those dealerships, such as AutoNation and Group One Automotive, rely on Liquid Motors' computer services to electronically market their inventory and in some cases maintain their websites.

12. Liquid Motors maintains duplicate servers to prevent any server outages and provide reliable computer inventory management and internet marketing to its customers. Liquid Motors houses its servers in a building on a five power grid with a generator that can last for thirty days. Those servers were also seized in the FBI raid.

13. If Liquid Motors' servers are down—as can occur only, for example, by a catastrophe to the building or here, where the FBI seized them—the automobile dealerships cannot manage their inventory, cannot market their products, and therefore lose sales. For example, upon information and belief, Group One Automotive's websites on the East Coast of the United States have been shut down by virtue of the seizure of Liquid Motors' computer equipment.

14. Liquid Motors had five different types of equipment at the Building: (1) Cisco networking devices; (2) computer servers; (3) storage arrays; (4) backup tapes; and (5) miscellaneous parts and pieces.

Cisco Networking Devices

15. There are six Cisco networking devices—two firewalls and four switches. The Cisco networking devices route network traffic to the appropriate servers and, through the firewalls, block traffic that is not authorized. The two firewalls of the Cisco networking devices are connected to internet access at the Building, and the four switches are connected to the firewalls.

16. There is no keyboard, monitor, or mouse access to the Cisco networking devices. The Cisco networking devices can only be accessed through a network or management device. When someone attempts to access the Cisco networking devices through a network or management device, the Cisco networking devices require a user identification and password, which rely on Keberos authentication for security.

17. The Cisco networking devices do not have a hard drive—documents and files are not stored on the networking devices. The only information to backup from the Cisco networking devices is the configuration of the networking device.

18. The Cisco networking devices may provide logs, which would be stored on the Cisco networking devices.

Computer Servers

19. There are fifteen computer servers. There are seven unique servers, one mirror image of each of those seven servers, and one test server. The servers are connected to the Cisco network and firewall.

20. The files on the servers consist of system files: operating systems, applications, and the configuration of the operating systems and applications. Liquid Motors stores no business data on the servers. However, several of the servers are critical to Liquid Motors' business because they are configured to access data on the storage arrays and recreating the configuration could take weeks.

21. The servers are divided into two groups—those that are accessible from the internet (the “DMZ Servers”) and those that are not (the “Corporate Servers”). Eight servers are Corporate Servers, which cannot be accessed from the internet and cannot be used to distribute content. Seven servers, including the test server, are DMZ Servers, and are accessible from the internet and can be used to distribute content.

22. The DMZ Servers may be accessed from the internet or network through four different protocols: http, https, ftp, and smtp. However, to put information or data on those servers requires a Keberos-authenticated user identification and password. The Corporate Servers cannot be accessed from the internet.

23. If someone attempted to physically access the DMZ Servers, they would have to shut down the servers and physically open the servers or they would have to go to the monitor and log in by breaking the Keberos-authenticated user identification and password. In the event that someone tried to open the servers, Liquid Motors would receive two notifications. First,

when the server is shut down, Liquid Motors would receive an email alert informing Liquid Motors that the server was shut down. In fact, Liquid Motors has received such email alerts in the past. However, Liquid Motors has investigated each email alert and validated that there was a legitimate reason that the server was shut down. This email alert notification cannot be disabled without first logging into the server or breaking into the Keberos-authenticated user identification and password protection.

24. Liquid Motors should also receive a second notification when someone opens the server. Liquid Motors uses Dell's OpenManage server management software, which monitors hardware failures and raises alerts for intrusion detection. Liquid Motors has received alerts through the OpenManage server for hardware failures, though not for intrusion, and has investigated each alert and determined that the servers had not been opened. The OpenManage intrusion detection feature cannot be disabled without first logging into the server or breaking into the Keberos-authenticated user identification and password protection.

25. The Keberos-authenticated user identification and password security, plus the shutdown and physical intrusion security, renders it highly improbable that someone could access Liquid Motors's computer servers.

26. Moreover, even if someone did access Liquid Motors's computer servers and were able to load files onto the system, such a person would have to reconfigure the firewalls and the servers to allow distribution of the files. This has not happened. Liquid Motors personally reviews the configuration on four of the seven DMZ servers (Web 01, Web 02, Web 03, and Web 72) at least three times per day. I have never noticed a change in configuration that cannot be attributed to modifications made by the staff of Liquid Motors. Of the remaining three DMZ

servers for which I do not review the configuration, one is not live and the other two are mail forwarding servers.

Storage Arrays

27. There are two storage arrays: a Dell AX100 and an EMC NS 352. Physical access to the storage arrays does not enable someone to place data on the storage arrays.

28. The Dell AX100 holds corporate email. The Dell AX100 is a Storage Attached Network ("SAN"), and is only accessible through the attached mail server. It cannot be accessed through the network; it must be physically attached to the mail server. Thus, for someone to gain access to the Dell AX100, they would need to first gain access to the mail server. Because the mail server is on the Corporate Server, information on the mail server cannot be disseminated on the internet without reconfiguring both the mail server and the Cisco networking device (which requires breaking two Keberos-authenticated passwords). Liquid Motors likely would have known about any such reconfiguration and is not aware of any such reconfiguration having occurred.

29. The EMC NS 352 contains all of the data used by Liquid Motors to perform its inventory management and marketing services to its automobile-dealership customers. This data includes pictures and inventory information.

30. The EMC NS 352 is divided into two pieces, a Network Attached Storage ("NAS") and Storage Attached Network ("SAN"). As discussed above, the SAN is accessible only through an attached server, here specifically the SQL server, which is on the internal, Corporate Server. The SQL server is not configured to disseminate information on the internet. Therefore, even if someone were to break into the Keberos-authenticated password and load files onto the SQL server, they would not be able to disseminate information loaded to the SQL server

without reconfiguring the SQL Server and Cisco networking device. Liquid Motors likely would have known about any such reconfiguration and is not aware of any such reconfiguration having occurred.

31. The NAS is accessible through the network, but only to the servers attached to the Liquid Motors's network. Access to the NAS, even though a network, is protected through a Keberos-authenticated user identification and password by the EMC Operating System, which is very secure, and significantly more difficult to penetrate than a Windows Operating System.

32. EMC monitors the EMC NS 352 storage array. If someone attempts to remove the hard drive from the EMC NS 352 storage array, the system will alert EMC which, in turn, will contact Liquid Motors. Liquid Motors has received alerts from EMC that a hard drive is having difficulties, but never that anyone removed a hard drive other than authorized Liquid Motors's employees or EMC employees.

Backup Tape Library

33. Liquid Motors also maintained a cycle of backup tapes for the storage array. Every night, the backup tape system runs a differential to detect and preserve any differences in the storage array. And, every week, the backup tape runs a full backup.

34. Most of the information on the storage array would have been contained on the backup tapes.

The Damage Being Done

35. Since the FBI seized Liquid Motors's computer equipment, Liquid Motors's business has been shut down. Liquid Motors has not been able to provide any contracted

services to customers. As a result, the business of Liquid Motors and, in turn, the employment of its approximately 20 employees is in severe jeopardy.

36. Liquid Motors's sole business is providing electronic inventory management and internet marketing to automobile dealerships. Liquid Motors cannot provide this service without the network devices, servers and storage arrays that have been seized. This computer equipment goes to the core of Liquid Motors's business.

37. The viability of Liquid Motors's business depends upon the prompt return of Liquid Motors's computer equipment—especially the servers and storage arrays. If Liquid Motors cannot obtain the immediate return of its computer servers and storage arrays, customers of Liquid Motors may seek to cancel their contracts with Liquid Motors causing Liquid Motors permanent and irreparable harm.

38. The property seized by the FBI and belonging to Liquid Motors amounts to approximately \$300,000 - \$400,000 of specialized computer equipment. The storage arrays, which have been seized, took eight weeks to order, deliver, install and configure. Although Liquid Motors is presently attempting to obtain replacement hardware, Liquid Motors cannot afford to replace all of the equipment—especially if Liquid Motors is precluded from conducting business while the FBI maintains all of the information contained on the storage arrays and servers.

39. Meanwhile, there is no basis to believe that the data contained on Liquid Motors storage arrays, servers, and other equipment has anything more than a remote chance of furthering the government's investigation.

40. This Complaint and request for emergency relief is brought solely to return Liquid Motors to the status quo prior the FBI's unlawful seizure of its property.

CAUSES OF ACTION

41. Liquid Motors incorporates the foregoing allegations as if fully set forth herein.

42. Liquid Motors sues Defendants under the Fourth and Fifth Amendments of the United States Constitution, and 42 U.S.C. § 1983. Defendants' conduct constitutes an illegal and unreasonable seizure under applicable law, a violation of Plaintiff's due process rights, and a taking without just compensation.

TEMPORARY RESTRAINING ORDER, TEMPORARY INJUNCTION, AND PERMANENT INJUNCTIVE RELIEF

43. Liquid Motors incorporates the foregoing allegations as if fully set forth herein.

44. Under Fed. R. Civ. P. 65, Plaintiff moves the Court for a temporary restraining order, temporary injunction, and permanent injunctive relief.

45. Plaintiff seeks injunctive relief requiring Defendants to:

- (1) Immediately return to Plaintiff Liquid Motors the storage arrays, servers and other equipment belonging to Plaintiff Liquid Motors;
- (2) Cease and desist from seizing any storage arrays, servers, and other equipment belonging to Plaintiff Liquid Motors; and
- (3) Cease and desist any activity that would prevent Liquid Motors from taking the steps necessary to ensure that its storage arrays, servers and equipment are operational.

Likelihood of Success on the Merits

46. The Constitution of the United States protects persons from unreasonable searches. The Fourth Amendment of the United States Constitution provides that:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. Unreasonable seizures of property are impermissible. “The touchstone of the Fourth Amendment is reasonableness.” *Florida v. Jimeno*, 500 U.S. 248, 251 (1991).

47. In this case, the United States seized the storage arrays, servers, and other equipment of Liquid Motors – conduct that is causing severe damage and likely the complete termination of Liquid Motors as a going concern. Such seizure – shutting down an innocent company, putting people out of work, and destroying investments – is not reasonable and is not permitted under the Constitution.

48. Meanwhile, the government cannot explain or will not share why it is necessary to keep Liquid Motors’ equipment. There is no evidence to suggest that such equipment, particularly the storage arrays and servers that are so critical to Plaintiffs’ business, has information relevant to the investigation. *See* Supp. Dec. of Daseke ¶¶ 15-18, 22-24 (explaining that in order for someone to access the storage arrays or servers, the person must first break into the Keberos-authenticated password protection and, in order for someone to distribute files to the internet, the person must reconfigure the servers and network devices which reconfiguration would have been detected by Liquid Motors).

49. Thus, under a reasonableness test, the seizure in this case was unreasonable. Therefore, Plaintiff has shown a likelihood of success on the merits.

Irreparable Harm and Inadequate Remedy at Law

50. Plaintiff will suffer and is suffering irreparable harm due to Defendants' conduct.

The Supplemental Declaration of Michael Daseke states as follows:

Since the FBI seized Liquid Motors's computer equipment, Liquid Motors's business has been shut down. Liquid Motors has not been able to provide any contracted services to customers. As a result, the business of Liquid Motors and, in turn, the employment of its approximately 20 employees is in severe jeopardy.

Liquid Motors's sole business is providing electronic inventory management and internet marketing to automobile dealerships. Liquid Motors cannot provide this service without the network devices, servers and storage arrays that have been seized. This computer equipment goes to the core of Liquid Motors's business.

The viability of Liquid Motors's business depends upon the prompt return of Liquid Motors's computer equipment—especially the servers and storage arrays. If Liquid Motors cannot obtain the immediate return of its computer servers and storage arrays, customers of Liquid Motors may seek to cancel their contracts with Liquid Motors causing Liquid Motors permanent and irreparable harm.

The property seized by the FBI and belonging to Liquid Motors amounts to approximately \$300,000 - \$400,000 of specialized computer equipment. The storage arrays, which have been seized, took eight weeks to order, deliver, install and configure. Although Liquid Motors is presently attempting to obtain replacement hardware, Liquid Motors cannot afford to replace all of the equipment—especially if Liquid Motors is precluded from conducting business while the FBI maintains all of the information contained on the storage arrays and servers.

See id. ¶¶ 27-30.

51. There is no adequate remedy at law. Liquid Motors is being put out of business because it cannot access its equipment. As explained above, a temporary restraining order is necessary to prevent permanent and irreparable harm to Liquid Motors and to restore the status quo until an injunction hearing can be held.

**MOTION FOR RETURN OF PROPERTY UNDER RULE 41(g)
AND BRIEF IN SUPPORT**

52. Liquid Motors also seeks return of its property under Federal Criminal Procedure Rule 41(g).

53. Rule 41(g) provides that: "A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. . . ."¹

54. As shown above, the equipment seized has little or no connection to this case and there is no evidence to suggest that it could be useful for Defendants' investigation.

55. Here, Defendants showed no regard for Plaintiff's property or rights and instead seized the property in violation of the Fourth and Fifth Amendments of the United States Constitution. Moreover, as shown in the Supplemental Declaration of Michael Daseke, Plaintiff has an interest and need of the property, would suffer irreparable injury without return of the property, and there is no adequate remedy at law. Thus, Plaintiff is entitled to relief under Rule 41(g).

¹ Under Rule 41(g), courts have considered the following factors in deciding whether to return property to a criminal being investigated pre-indictment:

- 1) whether the Government displayed callous disregard for constitutional rights;
- 2) whether the movant has an individual interest or need in the property;
- 3) whether the movant would suffer irreparable injury without return of the property; and
- 4) whether the movant has an adequate remedy at law.

In the Matter of Search of 5444 Westheimer Road Suite 1570 Houston, Texas on May 4, 2006, 2006 WL 1881370, *1 (S.D.Tex.) (citing *Richey v. Smith*, 515 F.2d 1279 (5th Cir. 1975)). This test does not apply here because it addresses parties that are trying to suppress and obtain the return of property from an illegal search, as a complement to the exclusionary rule, when they are a target of a governmental investigation. Although Plaintiff's circumstances satisfy this standard, this test has only been applied to those under investigation.

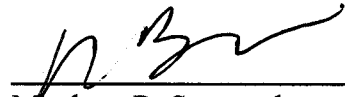
PRAYER

Wherefore, based on the foregoing, Plaintiff Liquid Motors requests that the Court

- (1) enter a temporary restraining order requiring that Defendants:
 - (i) Immediately return to Plaintiff Liquid Motors the storage arrays, servers and other equipment belonging to Plaintiff Liquid Motors;
 - (ii) Cease and desist from seizing any storage arrays, servers, and other equipment belonging to Plaintiff Liquid Motors; and
 - (iii) Cease and desist any activity that would prevent Liquid Motors from taking the steps necessary to ensure that its storage arrays, servers and equipment are operational.
- (2) enter a preliminary injunction and permanent injunctive relief in Plaintiff's favor;
- (3) grant Plaintiff's motion for the return of its property; and
- (4) grant Plaintiff its costs, attorneys' fees, and all such other relief to which it may be entitled.

Respectfully submitted,

VINSON & ELKINS L.L.P.



Matthew R. Stammel

State Bar No. 24010419

Frank C. Brame

State Bar No. 24031874

Michelle S. Spak

State Bar No. 24051363

Trammell Crow Center

2001 Ross Avenue, Suite 3700

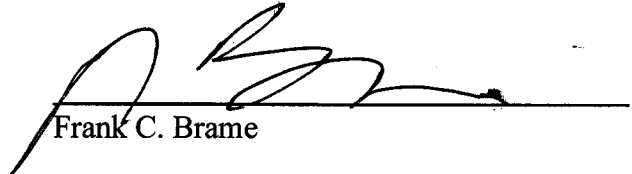
Dallas, TX 75201-2975

Telephone: (214) 220-7700

Facsimile: (214) 220-7716

CERTIFICATE OF SERVICE

I hereby certify that, on the 3rd day of April, 2009, I caused a true and correct copy of this filing to be sent by email to the United States Attorneys' Office of the Northern District of Texas.



Frank C. Brame

Dallas 1548870v.1

IN THE UNITED STATE DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

LIQUID MOTORS, INC.	§	
	§	
	§	CAUSE NO. 09-CV-0611-N
v.	§	
	§	
ALLYN LYND AND	§	
UNITED STATES OF AMERICA	§	

SUPPLEMENTAL DECLARATION OF MICHAEL DASEKE

STATE OF TEXAS	§
	§
COUNTY OF DALLAS	§

I, Michael Daseke, make this Declaration under the penalty of perjury under the laws of the United States:

1. My name is Michael Daseke. I am over eighteen years of age and I am fully competent to make this declaration. I have personal knowledge of the facts recited herein and declare such facts are true and correct.

2. I am President and Chief Executive Officer of Liquid Motors, Inc. ("Liquid Motors"). As President and Chief Executive Officer, I am knowledgeable about the technology and property used by Liquid Motors that is at issue in this matter.

3. Liquid Motors's business is to provide ongoing inventory management and internet marketing services to automobile dealerships throughout the country. Those dealerships, such as AutoNation and Group One Automotive, rely on Liquid Motors's computer services to electronically distribute their inventory and, in some cases, maintain their websites.

4. Liquid Motors maintains duplicate servers to prevent any server outages and provide reliable computer inventory management and internet marketing to its customers. Liquid Motors houses its servers in a building, located at 2323 Bryan Street, Dallas, Texas, on a five power grid with a generator that can last for thirty days. One of the only events that would shut down Liquid Motors's servers are a catastrophic event to the building in which the servers are housed or, as occurred here, seizure of all of Liquid Motors's equipment.

5. On April 2, 2009, the United States of America, acting through Special Agent Allyn Lynd of the Federal Bureau of Investigation seized property belonging to Liquid Motors, Inc. ("Liquid Motors"). At the time of the seizure, the property was contained in three racks in a cabinet located at 2323 Bryan St., Dallas, Texas (the "Building"), pursuant to a sublease Liquid Motors executed with Core IP Networks.

6. Liquid Motors had five different types of equipment at the Building: (1) Cisco networking devices; (2) computer servers; (3) storage arrays; (4) backup tapes; and (5) miscellaneous parts and pieces.

Cisco Networking Devices

7. There are six Cisco networking devices—two firewalls and four switches. The Cisco networking devices route network traffic to the appropriate servers and, through the firewalls, block traffic that is not authorized. The two firewalls of the Cisco networking devices are connected to internet access at the Building, and the four switches are connected to the firewalls.

8. There is no keyboard, monitor, or mouse access to the Cisco networking devices. The Cisco networking devices can only be accessed through a network or management device. When someone attempts to access the Cisco networking devices through a network or

management device, the Cisco networking devices require a user identification and password, which rely on Keberos authentication for security.

9. The Cisco networking devices do not have a hard drive—documents and files are not stored on the networking devices. The only information to backup from the Cisco networking devices is the configuration of the networking device.

10. The Cisco networking devices may provide logs, which would be stored on the Cisco networking devices.

Computer Servers

11. There are fifteen computer servers. There are seven unique servers, one mirror image of each of those seven servers, and one test server. The servers are connected to the Cisco network and firewall.

12. The files on the servers consist of system files: operating systems, applications, and the configuration of the operating systems and applications. Liquid Motors stores no business data on the servers. However, several of the servers are critical to Liquid Motors's business because they are configured to access data on the storage arrays and recreating the configuration could take weeks.

13. The servers are divided into two groups—those that are accessible from the internet (the “DMZ Servers”) and those that are not (the “Corporate Servers”). Eight servers are Corporate Servers, which cannot be accessed from the internet and cannot be used to distribute content. Seven servers, including the test server, are DMZ Servers, and are accessible from the internet and can be used to distribute content.

14. The DMZ Servers may be accessed from the internet or network through four different protocols: http, https, ftp, and smtp. However, to put information or data on those

servers requires a Keberos-authenticated user identification and password. The Corporate Servers cannot be accessed from the internet.

15. If someone attempted to physically access the DMZ Servers, they would have to shut down the servers and physically open the servers or they would have to go to the monitor and log in by breaking the Keberos-authenticated user identification and password. In the event that someone tried to open the servers, Liquid Motors would receive two notifications. First, when the server is shut down, Liquid Motors would receive an email alert informing Liquid Motors that the server was shut down. In fact, Liquid Motors has received such email alerts in the past. However, Liquid Motors has investigated each email alert and validated that there was a legitimate reason that the server was shut down. This email alert notification cannot be disabled without first logging into the server or breaking into the Keberos-authenticated user identification and password protection.

16. Liquid Motors should also receive a second notification when someone opens the server. Liquid Motors uses Dell's OpenManage server management software, which monitors hardware failures and raises alerts for intrusion detection. Liquid Motors has received alerts through the OpenManage server for hardware failures, though not for intrusion, and has investigated each alert and determined that the servers had not been opened. The OpenManage intrusion detection feature cannot be disabled without first logging into the server or breaking into the Keberos-authenticated user identification and password protection.

17. The Keberos-authenticated user identification and password security, plus the shutdown and physical intrusion security, renders it highly improbable that someone could access Liquid Motors's computer servers.

18. Moreover, even if someone did access Liquid Motors's computer servers and were able to load files onto the system, such a person would have to reconfigure the firewalls and the servers to allow distribution of the files. This has not happened. Liquid Motors personally reviews the configuration on four of the seven DMZ servers (Web 01, Web 02, Web 03, and Web 72) at least three times per day. I have never noticed a change in configuration that cannot be attributed to modifications made by the staff of Liquid Motors. Of the remaining three DMZ servers for which I do not review the configuration, one is not live and the other two are mail forwarding servers.

Storage Arrays

19. There are two storage arrays: a Dell AX100 and an EMC NS 352. Physical access to the storage arrays does not enable someone to place data on the storage arrays.

20. The Dell AX100 holds corporate email. The Dell AX100 is a Storage Attached Network ("SAN"), and is only accessible through the attached mail server. It cannot be accessed through the network; it must be physically attached to the mail server. Thus, for someone to gain access to the Dell AX100, they would need to first gain access to the mail server. Because the mail server is on the Corporate Server, information on the mail server cannot be disseminated on the internet without reconfiguring both the mail server and the Cisco networking device (which requires breaking two Keberos-authenticated passwords). Liquid Motors likely would have known about any such reconfiguration and is not aware of any such reconfiguration having occurred.

21. The EMC NS 352 contains all of the data used by Liquid Motors to perform its inventory management and marketing services to its automobile-dealership customers. This data includes pictures and inventory information.

22. The EMC NS 352 is divided into two pieces, a Network Attached Storage ("NAS") and Storage Attached Network ("SAN"). As discussed above, the SAN is accessible only through an attached server, here specifically the SQL server, which is on the internal, Corporate Server. The SQL server is not configured to disseminate information on the internet. Therefore, even if someone were to break into the Keberos-authenticated password and load files onto the SQL server, they would not be able to disseminate information loaded to the SQL server without reconfiguring the SQL Server and Cisco networking device. Liquid Motors likely would have known about any such reconfiguration and is not aware of any such reconfiguration having occurred.

23. The NAS is accessible through the network, but only to the servers attached to the Liquid Motors's network. Access to the NAS, even though a network, is protected through a Keberos-authenticated user identification and password by the EMC Operating System, which is very secure, and significantly more difficult to penetrate than a Windows Operating System.

24. EMC monitors the EMC NS 352 storage array. If someone attempts to remove the hard drive from the EMC NS 352 storage array, the system will alert EMC which, in turn, will contact Liquid Motors. Liquid Motors has received alerts from EMC that a hard drive is having difficult, but never that anyone removed a hard drive other than authorized Liquid Motors's employees or EMC employees.

Backup Tape Library

25. Liquid Motors also maintained a cycle of backup tapes for the storage array. Every night, the backup tape system runs a differential to detect and preserve any differences in the storage array. And, every week, the backup tape runs a full backup.

26. Most of the information on the storage array would have been contained on the backup tapes.

Harm to Liquid Motors

27. Since the FBI seized Liquid Motors's computer equipment, Liquid Motors's business has been shut down. Liquid Motors has not been able to provide any contacted services to customers. As a result, the business of Liquid Motors and, in turn, the employment of its approximately 20 employees is in severe jeopardy.

28. Liquid Motors's sole business is providing electronic inventory management and internet marketing to automobile dealerships. Liquid Motors cannot provide this service without the network devices, servers and storage arrays that have been seized. This computer equipment goes to the core of Liquid Motors's business.

29. The viability of Liquid Motors's business depends upon the prompt return of Liquid Motors's computer equipment—especially the servers and storage arrays. If Liquid Motors cannot obtain the immediate return of its computer servers and storage arrays, customers of Liquid Motors may seek to cancel their contracts with Liquid Motors causing Liquid Motors permanent and irreparable harm.

30. The property seized by the FBI and belonging to Liquid Motors amounts to approximately \$300,000 - \$400,000 of specialized computer equipment. The storage arrays, which have been seized, took eight weeks to order, deliver, install and configure. Although Liquid Motors is presently attempting to obtain replacement hardware, Liquid Motors cannot afford to replace all of the equipment—especially if Liquid Motors is precluded from conducting business while the FBI maintains all of the information contained on the storage arrays and servers.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed this 3rd day of April, 2009.



Michael Daseke

Dallas 1548868v.1